REMARKS

These remarks are set forth in response to the First Office Action. As this amendment has been timely filed within the three-month statutory period, neither an extension of time nor a fee is required. At the time of the First Office Action, Claims 1 through 21 were pending and rejected in this application. Independent Claims 1 and 8 have been amended to correct informalities in the naming convention and therefore are unrelated to patentability of the claimed subject matter.

CLAIMS 1-3, 8-10 AND 15-17 ARE REJECTED UNDER 35 U.S.C. § 102 AS BEING ANTICIPATED BY FRID, U.S. APPLICATION PUBLICATION NO. 2004/0030877 (HEREINAFTER FRID)

On page 2 of the First Office Action, the Examiner asserted that Frid discloses the invention corresponding to that claimed in Claims 1-3, 8-10 and 15-17. This rejection is respectfully traversed.

The factual determination of anticipation under 35 U.S.C. § 102 requires the identical disclosure, either explicitly or inherently, of each element of a claimed invention in a single reference.[1] Moreover, the anticipating prior art reference must describe the recited invention with sufficient clarity and detail to establish that the claimed limitations existed in the prior art and that such existence would be recognized by one having ordinary skill in the art.[2] As part of this analysis, the Examiner must (a) identify the elements of the claims, (b) determine the

[1] In re Rijckaert, 9 F.3d 1531, 28 USPQ2d 1955 (Fed. Cir. 1993); Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989); Perkin-Elmer Corp. v. Computervision Corp., 732 F.2d 888, 894, 221 USPQ 669, 673 (Fed. Cir. 1984).

[2] See In re Spada, 911 F.2d 705, 708, 15 USPQ 1655, 1657 (Fed. Cir. 1990); Diversitech Corp. v. Century Steps Inc., 850 F.2d 675, 678, 7 USPQ2d 1315, 1317 (Fed. Cir. 1988).

meaning of the elements in light of the specification and prosecution history, and (c) identify corresponding elements disclosed in the allegedly anticipating reference.[3] This burden has not been met.

<u>Claims 1-3, 8-10 and 15-17</u>

Claim 1 recites the following:

> A method for **reducing the boot time** of a Trusted Computing Performance Alliance (TCPA) based computing system comprising the steps of:
> resetting **said TCPA computing system**;
> executing a **boot block code** comprising a **Core Root of Trust for measurement (CRTM)**;
> reading **bits** in **a register** of a flash memory storing said boot block code, wherein **said bits in said register indicate whether segments of said flash memory have been updated**; and
> **obtaining** one or more **measurement values from a table storing hashed values** from a previous measurement of a Power On Self Test (POST) Basic Input/Output System (BIOS) if one or more of said bits read in said register indicate one or more of said segments of said flash memory storing said POST BIOS **have not been updated**.

On page 3 of the First Office Action, the Examiner relied upon paragraph [0022] and Figure 2, item 33 & item 34, and Figure 3, item 345 to teach these limitations. The passages are reproduced here for convenience.

> [0022] An embedded controller firmware image as well as **a firmware update algorithm or procedure are provided 31** as part of the BIOS. The computer system 10 is booted 32. During booting, or start-up, the system BIOS reads 33 **firmware identification data** from the embedded controller 21 and **compares it with corresponding data in the firmware image that is part of the BIOS**. This firmware identification data may be a fixed firmware validation signature, a checksum of the entire firmware image, a firmware version number, a firmware build time-stamp, or any other data that can identify embedded controller firmware 26. **Based on the comparison results, the system BIOS makes a decision 34 (see also FIG. 3) as to whether embedded controller firmware 26 should be updated.**

[3] <u>Lindermann Maschinenfabrik GMBH v. American Hoist & Derrick Co.</u>, 730 F.2d 1452, 221 USPQ 481 (Fed. Cir. 1984).

> Fig. 2, item block 33: during booting, reading firmware identification data from the embedded controller and comparing it with corresponding data in the system BIOS.
>
> Fig. 2, item block 34: **making a decision as to whether the embedded controller firmware should be updated** from the system BIOS image.
>
> Fig. 3, item block 345: is the firmware version number in the BIOS image equal to the firmware version number read from the embedded controller? (emphasis Applicants')

As claimed by Applicants, the method, system and computer program product for "**reducing the boot time** of a Trusted Computing Performance Alliance (TCPA) based computing system" includes "executing a **boot block code** comprising a **Core Root of Trust for measurement (CRTM)**". As an initial matter, there is no discussion or mention in Frid of "**reducing the boot time of a Trusted Computing Performance Alliance (TCPA) based computing system**" by "executing a **boot block code** comprising a **Core Root of Trust for measurement (CRTM)**". To the contrary, the Frid invention is specifically directed to a method that "implement[s] **embedded controller firmware updating**." (see paragraph [0005], lines 6-8, emphasis added). Moreover, Frid explicitly states that Figure 2 is a diagram "illustrating an exemplary **embedded controller firmware updating method 30** in accordance with the principles of the present invention." (see paragraph [0021], lines 1-4, emphasis added). Thus, paragraph [0022] and Figures 2 and 3 do not support the Examiner's conclusion that Frid discloses a method for "**reducing the boot time** of a ... **TCPA based** computing system".

The Examiner's second cited passage of Fig. 2, item block 33 refers to: "reading firmware identification data from the embedded controller and comparing it with corresponding data in the system BIOS." However, Fig. 2, item block 33 is silent as to where the "firmware identification data" resides and what the "firmware identification data" indicates. More importantly, there is no discussion in Frid of "**reading bits in a register** … wherein **said bits in said register indicate <u>whether segments</u> of said flash memory have been updated**". Instead of providing that the firmware of the embedded controller will be stored in multiple segments of flash memory, Frid explicitly teaches **<u>a single wholesale replacement of the embedded controller's firmware</u>**. (see paragraph [0026], lines 8-11; "new firmware image file … **<u>overwriting</u>** the existing firmware."). Thus, Fig. 2, item block 33 does not support the Examiner's conclusion of reading **bits** in **a register** of a flash memory storing said boot block code, wherein **said bits in said register indicate whether segments of said flash memory have been updated**.

The Examiner's third cited passage of Fig. 2, item block 34 and Fig. 3, item block 345 refers to: "**making a decision as to whether the embedded controller firmware should be updated** from the system BIOS image," and "is the firmware version number in the BIOS image equal to the firmware version number read from the embedded controller?" However, Fig. 2, item block 34 and Fig. 3, item block 345 are silent as to:

> **obtaining one or more measurement values** from a **table storing hashed values** from a **previous measurement** of a Power On Self Test (POST) Basic Input/Output System (BIOS) if one or more of **said bits in said register indicate one or more segments** of said flash memory storing said POST BIOS have not been updated.

There is no mention of "measurement values" in a "table storing hashed values" from a "**previous measurement** of a" POST BIOS if one or more of "**said bits in said register indicate one or more segments** of said flash memory storing said POST BIOS have not been updated." As such, the Examiner's cited passages **<u>do not support</u>** the Examiner's analysis.

The cited passages of Frid at paragraph [0022] and Figure 2, item 33 & item 34, and Figure 3, item 345 fail to teach or suggest a method, system and computer program product for reducing the boot time of a TCPA based computer system. The method, system and computer program product that executes "boot block code" that includes a CRTM, which are stored in the flash memory, where the flash memory is partitioned into multiple "segments" wherein each segment corresponds to a set of bits stored in a register, the bits in the register indicating whether segments of the flash memory have been updated. The method, system and computer program product can further include obtaining measurement values from a table storing hashed values from a previous measurement of a POST BIOS if one or more of the bits read in the register indicate the segments of the flash memory storing POST BIOS code have not been updated.

Consequently, Applicants' claimed invention advantageously reduces the boot time of a TCPA based computing system, since the CRTM does not need to perform a measurement of those segments of the POST BIOS identified as not having been updated, but instead can obtain measurement values from a table storing hashed values from a previous measurement of a POST BIOS. Frid, on the other hand, fails to even consider boot time in its "embedded controller firmware updating". Regardless of whether a decision is made to update the firmware of the embedded controller, to the extent that the Examiner maintains the position that the firmware update algorithm of the embedded controller corresponds to the Core Root of Trust for Measurement (CRTM) of the claimed invention, the Frid embedded controller would still be required to perform a measurement of **all** POST BIOS code during a reset of the Frid system, and thus incur substantial increases in boot time.

As a result, the cited passages of Frid at paragraph [0022] and Figure 2, item 33 & item 34, and Figure 3, item 345 fail to teach or suggest a method, system and computer program product for "**reducing the boot time** of a Trusted Computing Performance Alliance (TCPA) based computing system" that includes "executing a **boot block code** comprising a **Core Root of Trust for measurement (CRTM)**", "**reading bits in a register** … wherein **said bits in said register indicate** <u>**whether segments**</u> **of said flash memory have been updated**", and "obtaining one or more **measurement values** from a **table storing hashed values** from a **previous measurement of a POST BIOS** if one or more of the bits read in the register indicate the segments of the flash memory storing POST BIOS code have not been updated."

Thus, for the above-described reasons, the Examiner has failed to establish that Frid identically discloses the claimed invention, as recited in independent Claims 1, 8 and 15, within the meaning of 35 U.S.C. § 102(e). Applicants, therefore, respectfully submit that the imposed rejection of Claims 1, 8 and 15 under 35 U.S.C. § 102(e) for anticipation based on Frid is not factually viable and, hence, solicit withdrawal thereof.

<u>CLAIMS 4-7, 11-14 AND 18-21 ARE REJECTED UNDER 35 U.S.C. § 103 AS BEING UNPATENTABLE OVER FRID IN VIEW OF POLYUDOV, U.S. APPLICATION PUBLICATION NO. 2004/0186988 (HEREINAFTER POLYUDOV)</u>

Furthermore, the teachings of U.S. Application Publication No. 2004/0186988 to Polyudov (hereinafter Polyudov) cannot overcome the deficiencies of Frid, with respect to independent Claims 1, 8 and 15, and therefore Applicants respectfully request that the imposed rejection of Claims 4-7, 11-14 and 18-21 under 35 U.S.C. § 103 for obviousness based on Frid in view of Polyudov is not viable and, hence solicit withdrawal thereof.

For these reasons, the Applicants respectfully request the withdrawal of the rejections under 35 U.S.C. §§ 102(e) and 103(a). This entire application is now believed to be in condition for allowance and such action is respectfully requested. The Applicants request that the Examiner call the undersigned if clarification is needed on any matter within this Amendment, or if the Examiner believes a telephone interview would expedite the prosecution of the subject application to completion.

Respectfully submitted,

Date: November 9, 2007

/Steven M. Greenberg/

Steven M. Greenberg
Reg. No.: 44,725
Customer Number 50594
Attorney for Applicant(s)
Carey, Rodriguez, Greenberg & Paul, LLP
950 Peninsula Corporate Circle, Suite 3020
Boca Raton, FL 33487
Tel: (561) 922-3845
Fax: (561) 244-1062